AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF CLAIMS

1.   (Currently Amended)   A method for cryptographically processing data, said method comprising:

receiving a plurality of data segments;

selecting, for each data segment, a set of encryption information for a current data segment to be encrypted based on data contained in a predetermined portion of the current data segment to be encrypted; and

encrypting the current each data segment using the set of encryption information selected for the current data segment; and

repeating said selecting and said encrypting for subsequent data segments.

2.   (Currently Amended)   The method of claim 1, wherein said selecting comprising:

changing at least one of an encryption algorithm, an encryption key, and an encryption parameter for each current data segment based on the data contained in the predetermined portion of the current data segment.

3.   (Currently Amended)   The method of claim 1, wherein said selecting comprises:

generating, for each current data segment, a value from data contained in the predetermined portion of the current data segment; and

selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

4.   (Original)   The method of claim 3, wherein said generating a value comprises:

hashing the data contained in the predetermined portion using a hash key.

3

5.   (Original)   The method of claim 3, further comprising:

providing an encryption table containing:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a generate value.

6.   (Original)   The method of claim 1, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter.

7.   (Original)   The method of claim 6, wherein said receiving comprises:

receiving a data stream including a plurality of data packets, each data packet corresponding to a data segment.

8.   (Original)   The method of claim 7, wherein the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

9.   (Original)   The method of claim 7, wherein the first predetermined portion is an Internet Protocol (IP) header of the data packet.

10.   (Currently Amended)   The method of claim 9, wherein the second predetermined portion is either one of:

    a selected portion of a data field of the data packet; ~~packet~~

    a Transmission Control Protocol (TCP) header of the data packet; and

    a User Datagram Protocol (UDP) header of the data packet.

11-12. (Cancelled)

13.   (Original)   The method of claim 6, wherein said receiving comprises:

    reading the plurality of data segments from corresponding sectors in a data storage device.

14.   (Original)   The method of claim 13, wherein the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

15.   (Original)   The method of claim 6, further comprising:

    encrypting the second predetermined portion using the first set of encryption information.

16.   (Original)   The method of claim 15, further comprising:

    encrypting the remaining portion of the data segment using the second set of encryption information.

17.   (Original)   The method of claim 16, further comprising:

    generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment.

5

18.   (Original)   The method of claim 17, further comprising:

transmitting a plurality of encrypted data segments as a stream of encrypted data.

19.   (Original)   The method of claim 17, further comprising:

storing a plurality of encrypted data segments on a data storage device, each encrypted data segment corresponding to a respective data sector of the data storage device.

20.   (Original)   The method of claim 17, further comprising:

receiving the encrypted data including a plurality of encrypted data segments;

selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment;

decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment;

selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion; and

decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment.

21.   (Original)   The method of claim 20, wherein said selecting the first encryption information comprises:

generating a first value from the original data contained in the first predetermined portion of the encrypted data segment.

22.   (Original)   The method of claim 21, wherein said generating the first value comprises:

hashing the data contained in the first predetermined portion using a first hash key.

23. (Original) The method of claim 20, wherein said selecting the second encryption information comprises:

generating a second value from the decrypted data of the second predetermined portion of the encrypted data segment.

24. (Original) The method of claim 23, wherein said generating the second value comprises:
hashing the decrypted data of the second predetermined portion using a second hash key.

25. (Currently Amended) A method for cryptographically processing data, said method comprising:

receiving a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion;

selecting, for each encrypted data segment, a set of encryption information for a current encrypted data segment to be decrypted based on data contained in the predetermined portion of the current encrypted data segment; and

decrypting the current each encrypted data segment using the encryption information selected for the current encrypted data segment; and

repeating said selecting and said decrypting for subsequent encrypted data segments.

26. (Currently Amended) The method of claim 25, wherein said selecting comprises:

generating, for each current encrypted data segment, a value from data contained in the predetermined portion of the current encrypted data segment; and

selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

27. (Original) The method of claim 26, wherein said generating a value comprises:
hashing the data contained in the predetermined portion using a hash key.

28.   (Original)   The method of claim 27, further comprising:

providing an encryption table, the encryption table containing:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a generated value.

29.   (Original)   The method of claim 25, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter.

30.   (Original)   The method of claim 29, wherein said receiving comprises:

receiving an encrypted data stream including a plurality of encrypted data packets, each encrypted data packet corresponding to an encrypted data segment.

31.   (Original)   The method of claim 30, wherein the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

32.   (Original)   The method of claim 30, wherein the first predetermined portion is an Internet Protocol (IP) header of the data packet.

33.   (Currently Amended)   The method of claim 32, wherein the second predetermined portion is either one of:

a selected portion of a data field of the data packet: packet

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

8

34-35.   (Cancelled)

36.   (Original)   The method of claim 29, wherein said receiving comprises:

reading the plurality of encrypted data segments from corresponding sectors in a data storage device.

37.   (Original)   The method of claim 36, wherein the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

38.   (Original)   The method of claim 29, wherein data contained in the second predetermined portion of the encrypted data segment has been encrypted using the first set of encryption information.

39.   (Original)   The method of claim 38, wherein data contained in the remaining portion of the encrypted data segment has been encrypted using the second set of encryption information.

40.   (Currently Amended)   An apparatus for cryptographically processing data, comprising:

an input buffer adapted to receive data including a plurality of data segments;

an encryption module adapted to encrypt each data segment;

a controller coupled to said input buffer and said encryption module, said controller being adapted to select a set of encryption information for a current ~~each~~ data segment to be encrypted based on data contained in a predetermined portion of the current data segment ~~to be encrypted~~; and

an output buffer coupled to said controller and said encryption module, said output buffer being adapted to output encrypted data including a plurality of encrypted data segments.

41.   (Original)   The apparatus of claim 40, wherein said controller changes at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment.

42.   (Currently Amended)   The apparatus of claim 40, wherein said encryption module comprises:

a plurality of encryption engines, each encryption engine corresponding to a respective encryption algorithm different from each other.

43.   (Original)   The apparatus of claim 40, wherein said encryption module further comprises:

a data buffer coupled to each of the plurality of encryption engines.

44.   (Original)   The apparatus of claim 40, wherein said controller comprises:

a data selector adapted to select a predetermined portion of each data segment;

an encryption selector coupled with said data selector, adapted to select a set of encryption information in accordance with data contained in the predetermined portion, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter; and

an encryption controller adapted to select and activate an encryption engine based on the encryption information.

45.   (Original)   The apparatus of claim 40, wherein said controller further comprises:

a value generator coupled to said data selector, adapted to generate a value from the data contained in the predetermined portion.

46.   (Original)   The apparatus of claim 45, wherein said value generator is adapted to hash the data contained in the predetermined portion using a hash key.

47.   (Original)   The apparatus of claim 45, wherein said encryption controller comprises an encryption table containing:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a generated value.

48.   (Original) The apparatus of claim 40, wherein the predetermined portion of each data segment comprises:

a first predetermined portion; and

a second predetermined portion.

49.   (Original) The apparatus of claim 48, wherein the plurality of data segments are data packets in a data stream.

50.   (Original) The apparatus of claim 49, wherein the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

51.   (Original) The apparatus of claim 49, wherein the first predetermined portion is an Internet Protocol (IP) header of the data packet.

52.   (Currently Amended) The apparatus of claim 51, wherein the second predetermined portion is either one of:

a selected portion of a data field of the data packet: ~~packet~~

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

53-54. (Cancelled)

55.   (Original) The method of claim 48, wherein the plurality of data segments are sectors in a data storage device.

56.   (Original)   The apparatus of claim 55, wherein the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

57.   (Original)   The apparatus of claim 48, wherein said controller comprises:

a first encryption table for selecting the first set of encryption information based on data contained in the first predetermined portion; and

a second encryption table for selecting the second set of encryption information based on data contained in the second predetermined portion.

58.   (Currently Amended)   An apparatus for cryptographically processing data, comprising:

an input buffer adapted to receive a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion;

an encryption module adapted to decrypt each encrypted data segment;

a controller coupled to said input buffer and said decryption module, said controller being adapted to select a set of encryption information for a current ~~each~~ encrypted data segment to be decrypted based on data contained in a predetermined portion of the current encrypted data segment; and

an output buffer coupled to said controller and said decryption module, said output buffer being adapted to output decrypted data including a plurality of decrypted data segments.

59.   (Currently Amended)   The apparatus of claim 58, wherein said decryption module comprises:

a plurality of decryption engines, each decryption engine corresponding to a respective encryption algorithm different from each other.

60.   (Original)   The apparatus of claim 58, wherein said decryption module further comprises:

a data buffer coupled to each of the plurality of decryption engines.

61.   (Original)   The apparatus of claim 58, wherein said controller comprises:

a data selector adapted to select a predetermined portion of each encrypted data segment;

a decryption selector coupled with said data selector, adapted to select a set of decryption information in accordance with data contained in the predetermined portion, the set of decryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter; and

a decryption controller adapted to select and activate a decryption engine based on the encryption information.

62.   (Original)   The apparatus of claim 58, wherein said controller further comprises:

a value generator coupled to said data selector, adapted to generate a value from the data contained in the predetermined portion.

63.   (Original)   The apparatus of claim 62, wherein said value generator is adapted to hash the data contained in the predetermined portion using a hash key.

64.   (Original)   The apparatus of claim 62, wherein said decryption controller comprises an encryption table containing:

an encryption type identifier;

an encryption key for the encryption type; and

an encryption parameter,

for each entry associated with a generated value.

65.   (Original)   The apparatus of claim 58, wherein the predetermined portion of each data segment comprises:

a first predetermined portion; and

a second predetermined portion.

66.   (Original)   The apparatus of claim 65, wherein the plurality of data segments are data packets in a data stream.

67.   (Original)   The apparatus of claim 66, wherein the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

68.   (Original)   The apparatus of claim 66, wherein the first predetermined portion is an Internet Protocol (IP) header of the data packet.

69.   (Currently Amended)   The apparatus of claim 68, wherein the second predetermined portion is either one of:

        a selected portion of a data field of the data packet: packet

        a Transmission Control Protocol (TCP) header of the data packet; and

        a User Datagram Protocol (UDP) header of the data packet.

70-71. (Cancelled)

72.   (Original)   The method of claim 58, wherein the plurality of data segments are sectors in a data storage device.

73.   (Original)   The apparatus of claim 72, wherein the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

74.   (Original)   The apparatus of claim 58, wherein said controller comprises:

        a first encryption table for selecting the first set of decryption information based on data contained in the first predetermined portion; and

        a second encryption table for selecting the second set of decryption information based on data contained in the second predetermined portion.

75.   (Currently Amended)   An apparatus for cryptographically processing data, said apparatus comprising:

means for receiving a plurality of data segments;

means for selecting, for each data segment, a set of encryption information for a current data segment to be encrypted based on data contained in a predetermined portion of the current data segment to be encrypted; and

means for encrypting the current each data segment using the set of encryption information selected for the current data segment; and

means for allowing said means for selecting and said means for encrypting to operate on subsequent data segments.

76.   (Original)   The apparatus of claim 75, wherein said means for selecting changes at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment based on the data contained in the predetermined portion.

77.   (Currently Amended)   The apparatus of claim 75, wherein said means for selecting comprises:

means for generating, for each current data segment, a value from data contained in the predetermined portion of the current data segment; and

means for selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

78.   (Original)   The apparatus of claim 77, wherein said means for generating a value comprises:

means for hashing the data contained in the predetermined portion using a hash key.

79.   (Original)   The apparatus of claim 77, further comprising:

means for providing an encryption type identifier, an encryption key for the encryption type, and an encryption parameter associated with a generate value.

80.   (Original) The apparatus of claim 75, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter.

81.   (Original) The apparatus of claim 80, further comprising:

means for encrypting the second predetermined portion using the first set of encryption information.

82.   (Original) The apparatus of claim 81, further comprising:

means for encrypting the remaining portion of the data segment using the second set of encryption information.

83.   (Original) The apparatus of claim 82, further comprising:

means for generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment.

84.   (Original) The apparatus of claim 83, further comprising:

means for transmitting a plurality of encrypted data segments as a stream of encrypted data.

85.   (Original)   The apparatus of claim 83, further comprising:

means for storing a plurality of encrypted data segments on a data storage device, each encrypted data segment corresponding to a respective data sector of the data storage device.

86.   (Original)   The apparatus of claim 83, further comprising:

means for receiving the encrypted data including a plurality of encrypted data segments;

means for selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment;

means for decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment;

means for selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion; and

means for decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment.

87.   (Original)   The apparatus of claim 86, wherein said means for selecting the first encryption information comprises:

means for generating a first value from the original data contained in the first predetermined portion of the encrypted data segment.

88.   (Original)   The apparatus of claim 87, wherein said means for generating the first value comprises:

means for hashing the data contained in the first predetermined portion using a first hash key.

89.   (Original)   The apparatus of claim 86, wherein said means for selecting the second encryption information comprises:

means for generating a second value from the decrypted data of the second predetermined portion of the encrypted data segment.

17

90.   (Original)   The apparatus of claim 89, wherein said means for generating the second value comprises:

means for hashing the decrypted data of the second predetermined portion using a second hash key.

91.   (Currently Amended)   An apparatus for cryptographically processing data, said apparatus comprising:

means for receiving a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion;

means for selecting, for each encrypted data segment, a set of encryption information for a current encrypted data segment to be decrypted based on data contained in the predetermined portion of the current encrypted data segment; and

means for decrypting the current each encrypted data segment using the encryption information selected for the current encrypted data segment; and

means for allowing said means for selecting and said means for decrypting to operate on subsequent encrypted data segments.

92.   (Currently Amended)   The apparatus of claim 91, wherein said means for selecting comprises:

means for generating, for each current encrypted data segment, a value from data contained in the predetermined portion of the current encrypted data segment; and

means for selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

93.   (Original) The apparatus of claim 92, wherein said means for generating a value comprises:

means for hashing the data contained in the predetermined portion using a hash key.

94.   (Original)   The apparatus of claim 93, further comprising:

means for providing an encryption type identifier, an encryption key for the encryption type, and an encryption parameter associated with a generated value.

95. (Original) The apparatus of claim 91, wherein the predetermined portion comprises:
a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter; and
a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter.

96. (Original) The apparatus of claim 95, wherein data contained in the second predetermined portion of the encrypted data segment has been encrypted using the first set of encryption information.

97. (Original) The apparatus of claim 96, wherein data contained in the remaining portion of the encrypted data segment has been encrypted using the second set of encryption information.